Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Modernizing the E-Rate Program for Schools and Libraries	)	WC Docket No. 13-184
	)	
	)	
Wireline Competition Bureau Seeks Comment On Proposed Eligible Services List for The E-Rate Program	)	
	)	
	)	

COMMENTS OF COX COMMUNICATIONS, INC.

Cox Communications, Inc., ("Cox") hereby submits these comments in response to the Wireline Competition Bureau's ("Bureau") public notice regarding the proposed Eligible Services List ("ESL") for funding year 2020.[1] Cox urges the Bureau to include network security equipment and services to prevent and recover from cyberattacks on the ESL for funding year 2020.[2] Although the Commission declined to include E-Rate support for "further network security services," such as Direct Denial of Service ("DoS") attack prevention and mitigation services, in the 2014 Modernization Order,[3] it did so without significant deliberation or a robust record. Since that time, based on informal feedback from our educational customers and online news sources, schools across the country have experienced a marked increase in the number of ransomware and DDoS attacks,[4] which warrants a fresh look at network security services.

---

[1] Wireline Competition Bureau Seeks Comment on Proposed Eligible Services List for the E-Rate Program, DA 19-738 (WCB. rel. Aug. 2, 2019).

[2] Cox also supports the Commission's proposal to make permanent funding for category 2 internal connections, managed internal broadband services, caching, and basic maintenance of internal connections. *See* Cox Comments filed in response to *Modernizing the E-Rate Program for Schools and Libraries*, Notice of Proposed Rulemaking, FCC 19-58 (rel. July 9, 2019).

[3] *See Modernizing the E-Rate Program for Schools and Libraries*, Report and Order and Further Notice of Proposed Rulemaking, 29 FCC Rcd 8870, 8918, para 121 & n. 275 ("*Modernization Order*") (declining to designate services suggested by commenters, including intrusion protection and detection, malware protection, application control, content filters, DDoS mitigation, and cybersecurity services, as eligible in three sentences).

[4] *See, e.g.*, "Louisiana Governor declares emergency after ransomware attack hits three schools," https://cyware.com/news/louisiana-governor-declares-emergency-after-ransomware-attack-hits-three-schools-50569756; "New Haven Public Schools hit with ransomware attack," https://cyware.com/news/new-haven-public-schools-hit-with-ransomware-attack-7079b9a7; "Syracuse Schools, Libraries Disabled by Ransomware Attack," https://www.govtech.com/education/Syracuse-Schools-Libraries-Disabled-by-Ransomware-Attack.html?utm_term=READ%20MORE&utm_campaign=New%20York%20School%20District%20Changes%20Facial%20Recognition%20Policy&utm_content=email&utm_source=Act-On+Software&utm_medium=email; "Connecticut School District Hit with Ransomware Attack," https://www.govtech.com/security/Connecticut-School-District-Hit-with-Ransomware-Attack.html; "Ransomware attack on Oklahoma City Public Schools,"

The challenges facing school and library system information technology ("IT") departments across the country have grown aggressively since 2014, while IT budgets have faced increasing pressure.[5] At the same time IT budgets are squeezed in the education space, the complexity of technology, the diversity of skills needed to support it and the threats to networks, sensitive data and operations systems are expanding at an exponential rate. As such, an effective means of addressing this exposure is to enlist the assistance of companies that can provide the software, equipment, services and personnel to secure the school system's IT operations and possibly provide those things in an as-a-service, operating expense format. Unfortunately, without the support of E-Rate, the funds for such services aren't in the typical school system's budget.

A DDoS attack is an attempt from an outside individual or group to overload network systems, equipment and memory resources. DDoS attacks are unique from other types of malware or viruses, because they do not simply slow down Internet service; they can cripple systems and effectively result in a temporary loss of Internet service. In addition, certain types of reflective DDoS attacks[6] can saturate Internet broadband circuits, leaving local firewall appliances helpless to restrict unwanted traffic. Ransomware is a type of malware that locks a target's files, date or the PC itself and extorts money in order to provide access. Available DDoS and Ransomware services include monitoring school and library networks for DDoS attacks and malware and mitigation of attacks by filtering out unwanted traffic. Products and services that mitigate malware, including ransomware, would include, for example, a next generation firewall, which includes intrusion detection, AV Malware protection, and content filtering; end point protection, such as AV malware software installed on a PC or MAC; and a recursive DNS firewall.

---

https://www.cybersecurity-insiders.com/ransomware-attack-on-oklahoma-city-public-schools/; "Coventry Public Schools' computers attacked with malware," https://turnto10.com/i-team/nbc-10-i-team-coventry-public-schools-computers-attacked-with-malware?fbclid=IwAR3s6UePp-OB5ZqdM2lGsp__Mevi7s31uOt5HGg0PKa2BO4kx27ZKDl3VWU, "Back to School DDoS Attacks Blocks Parents and Students Across the U.S.," https://www.secureworldexpo.com/industry-news/ddos-attack-example; "DDoS-for-Hire Services Doubled in Q1," https://www.darkreading.com/perimeter/ddos-for-hire-services-doubled-in-q1-/d/d-id/1335042.

[5] Most public school systems have seen operating budgets grow at a rate that barely overcomes inflation and have seen a reduction in payrolls that would support internal IT operational capacity. According to the National Center for Educational Statistics (NCES), since the year 2000, the percentage of budget allocated to payroll has fallen 7% (from 64% to 57%) while both employee benefits and purchased services has risen over the same period. *See* https://nces.ed.gov/programs/coe/indicator_cmb.asp.

[6] A reflective attack may involve sending forged requests to a large number of computers that will reply to the requests and send those replies to the targeted victim through the use of Internet Protocol address spoofing.

Because DDoS and ransomware attacks can render Internet service effectively unusable, support for DDoS and ransomware prevention and restoration services and equipment is necessary to protect the E-Rate fund's investment in Internet access, internal connections, and the integrity of educational networks.[7] The Commission's first goal in modernizing the E-Rate program was "ensuring affordable access to high-speed broadband sufficient to support digital learning in schools and robust connectivity for all libraries."[8] Inclusion of DDoS and ransomware attack prevention and mitigation equipment and services will further this goal by ensuring that schools and libraries have the protection necessary for continued access to the high-speed services made possible by the E-Rate program.[9] If demand for network security solutions becomes unreasonably high, the Commission can always adopt measures to prioritize or cap requests for such services, or as it has before, track spending trends and revisit if new demand reaches a certain percentage of overall E-Rate support.

The Commission should also clarify that E-Rate should provide support for equipment and services, including virtualized services, which perform cybersecurity asset protection and restoration functions. Provided the function that the virtualized solution performs is eligible, the fact that it is associated with a cloud-based solution, not a hardware-based solution, should be irrelevant. Virtualized solutions may be preferred or more cost-effective than their hardware-based equivalents, when taking into account equipment maintenance, down time and equipment obsolescence, and should be an option for schools and libraries. For the same reasons, the Commission should no longer restrict support to virtualized eligible internal connections, rather

---

[7] Recently, other parties have also suggested making E-Rate support available for cybersecurity services and equipment in other dockets. *See* Telesolutions Consultants LLC comments to Notice of Proposed Rulemaking, *Universal Service Contribution Methodology*, FCC 19-46, WC Docket No. 06-122 (July 25, 2019); Comments filed in response to Notice of Proposed Rulemaking, *Modernizing E-Rate Program for Schools and Libraries*, WC Docket No. 13-184 by State E-Rate Coordinators' Alliance and Schools, Health & Libraries Broadband Coalition (Aug. 16, 2019), Funds for Learning LLC (Aug. 16, 2019), Aruba – Hewlett Packard Enterprise company (Aug. 16, 2019), Cisco Systems, Inc. (Aug. 16, 2019), New Mexico Public School Facilities Authority (Aug. 16, 2019), Education Superhighway (Aug. 16, 2019), Infinity Communications & Consulting, Inc. (Aug. 16, 2019), E-Rate Management Professionals Assoc. (Aug. 16, 2019), Fortinet, Inc. (Aug. 15, 2019); Reply Comments filed in response to *Modernizing E-Rate Program for Schools and Libraries* Notice of Proposed Rulemaking by Council of Chief State School Officers (Sept. 3, 2019), Illinois Department of Innovation and Technology (Sept. 3, 2019); State Educational Technology Directors Association (Sept. 3, 2019); Education SuperHighway (Sept. 3, 2019).

[8] *2014 First E-Rate Order*, 29 FCC Rcd at 8881, para. 26.

[9] Network security services that protect against and help systems recover from DDoS and Ransomware attacks protect assets used to provide internal connections and could be considered category two expenses. However, they also protect assets used to provide Internet access, so they could alternatively be funded under category one. In either case, support would protect assets purchased with E-Rate funds.

it should support virtualized equivalents of eligible category one and category two equipment and services.

Based on the reasons outlined herein, Cox respectfully requests that the Bureau include network security solutions to prevent and mitigate ransomware and DDoS attacks on the ESL for funding year 2020.

Respectfully submitted.

By: _____/s/_____

Joiava Philpott
Vice President, Regulatory Affairs
Cox Communications, Inc.
6205 Peachtree Dunwoody Road
Atlanta, GA 30328

September 9, 2019